Groups Generated by Two Operators Whose Relative Transforms are Equal to Each Other.

BY G. A. MILLER.

If s and t represent two operators of a group the important operator

$$s^{-1}ts$$

is known as the *transform* of t with respect to s. Similarly $t^{-1}st$ is called the transform of s with respect to t. These two transforms are usually distinct. When s and t are commutative they are equal to each other whenever s and t are identical and only then. When s and t are non-commutative the equality of these transforms still implies, among other things, that s and t have the same order, since the order of an operator is equal to that of all its transforms. The main object of the present paper is to determine fundamental properties of the groups generated by s and t when they satisfy the equation

$$s^{-1}ts=t^{-1}st, \tag{A}$$

but are not otherwise restricted.

Our first object is to determine the order of $t^{-1}s$ when the common order of s and t is an arbitrary positive integer α. For the determination of this order it is convenient to employ the equation

$$(t^{-1}s)^2=st^{-1}, \tag{B}$$

which can readily be established by writing (A) in the form

$$t^{-1}s=s^{-1}tst^{-1},$$

and substituting in the second member of

$$(t^{-1}s)^2=t^{-1}st^{-1}s.$$

From (B) it results directly that $t^{-1}s$ is transformed into its square by s^{-1}. Hence s transforms into itself the cyclic group generated by $t^{-1}s$, and the group G generated by this cyclic group and s is identical with the group generated by s and t. In particular, it results that G is of finite order provided $t^{-1}s$ is of finite order. We shall now prove that the latter order is a divisor of

$$2^{\alpha}-1=2^{\alpha-1}+2^{\alpha-2}+\ldots\ldots+2+1.$$

This fact can easily be established by means of (B). When $\alpha=1$ no proof is required. When $\alpha>1$, sets of four factors in the first member of the following equation, beginning at the left,

$$t^{-1}st^{-1}s\ldots.t^{-1}s=(t^{-1}s)^{2\alpha-1}$$

can be replaced by sets of two factors by means of (B). We thus obtain the simpler equation

$$st^{-1}st^{-1}\ldots.t^{-2}s=(st^{-1})^{2\alpha-1-1}\cdot t^{-1}s=s(t^{-1}s)^{2\alpha-1-2}\cdot t^{-2}s.$$

When $\alpha=2$ it is evident that the members of the last equation reduce to identity. When $\alpha>2$ we may write out the last member of this equation and in it affect a similar reduction by means of (B), thus obtaining the equation

$$s^2t^{-1}st^{-1}s\ldots.t^{-3}s=s^2(t^{-1}s)^{2\alpha-2-2}\cdot t^{-3}s.$$

The members of this equation are evidently equal to the identity when $\alpha=3$. When $\alpha>3$ the process may clearly be repeated until the identity is reached. Hence the theorem:

If s and t are two operators of order α which satisfy the condition $s^{-1}ts=t^{-1}st$, then the order of $t^{-1}s$ is a divisor of $2^\alpha-1$.

The fact that the order of $t^{-1}s$ must be exactly $2^\alpha-1$ whenever no additional restriction is placed on s and t, may be established by actually constructing a group involving operators which satisfy these conditions. We proceed to do this. Let t_1 represent an operator of order $2^\alpha-1$ and let s_1 represent an operator of order α in the group of isomorphisms of the cyclic group generated by t_1. Since 2 belongs to exponent α mod $2^\alpha-1$ it may be assumed that $s_1t_1s_1^{-1}=t_1^2$, and hence

$$t_1s_1^{-1}t_1^{-1}=s_1^{-1}t_1.$$

The operators s_1 and $s_1t_1^{-1}$ are therefore of order α. Their relative transforms are equal to each other since

$$s_1^{-1}\cdot s_1t_1^{-1}s_1=t_1^{-1}s_1 \text{ and } t_1s_1^{-1}\cdot s_1\cdot s_1t_1^{-1}=t_1s_1t_1^{-1}.$$

In fact, the second members of these two equations are the inverses of operators which were proved equal to each other and hence they must also be equal to each other.

From the preceding paragraph it results that there are two operators of order α, α being any positive integer, whose relative transforms are equal to each other and which satisfy the condition that the product of one and the inverse of the other is of order $2^\alpha-1$. Hence the following theorem has been established:

If the relative transforms of two operators of a group are equal to each other these operators have the same order α and when they are not otherwise restricted they generate a solvable group of order α $(2^{\alpha}-1)$.

For a particular value of α there is one and only one such group. This group contains a cyclic commutator subgroup of order $2^{\alpha}-1$ and is generated by this subgroup and an operator of order α which transforms each of its operators into its square. In view of the great importance of the concept of transform in the theory of groups and the remarkable simplicity of these groups it may be desirable to denote this system by a special name. We shall call it the *equi-transform system* of groups.

For the sake of illustrations it may be desirable to note that when $\alpha=1$ this group is the identity, when $\alpha=2$ it is the dihedral group of order 6, when $\alpha=3$ it is the semi-metacyclic group of order 21, etc. It is evident that each of the groups in the equi-transform system contains a set of $2^{\alpha}-1$ conjugate cyclic subgroups of order α which are therefore separately transformed into themselves by only their own operators. Moreover, when α is even and represented by $2n$ all the $2^{n}+1$ operators of order 2 contained in such a group constitute a single set of conjugates. The fact that each of these operators of order 2 appears in at least one set of independent generators of G results directly from the following evident theorem:

If each one of a complete set of conjugate operators of a group can be transformed into each of the other operators of the set by some operator of the set then each of these operators appears in at least one set of independent generators of the group.

From the preceding paragraph it results directly that the ϕ-subgroup of G must always be of odd order. We proceed to prove that the order of this subgroup is $2^{\alpha}-1$ divided by the product of all its distinct prime factors. To prove this theorem it is only necessary to prove that every operator of G which is not found in its invariant cyclic subgroup of order $2^{\alpha}-1$ does appear in at least one of the sets of independent generators of G. If this theorem were not true there would be such an operator S of prime order p which would not belong to a set of conjugates having the properties noted in the theorem closing the preceding paragraph.

Since S would be a power of an operator s of order α contained in G it may be assumed that $\alpha=kp$ and that $s^{-1}ts=t^{2}$, t being a generator of the invariant cyclic subgroup of order $2^{\alpha}-1$ contained in G. Hence

$$S^{-1}tS=t^{2^{k}}.$$

It may be noted that when $2^{\alpha}-1$ is prime to p the theorem is evident. Hence we shall assume in what follows that $2^{\alpha}-1$ is divisible by p. Moreover, it may be assumed that S is commutative with the Sylow subgroups whose orders are prime to p contained in the invariant cyclic subgroup of order $2^{\alpha}-1$. Hence it results that

$$2^k-1\equiv 0 \mod (2^{\alpha}-1)/p.$$

It is easy to prove that this congruence is impossible. In fact,

$$p(2^k-1)<2^{\alpha}-1$$

since $p\cdot 2^k<2^{\alpha}=2^{kp}$. Hence the operator S belongs to a set of conjugates such that each of the operators of the set is transformed into every operator of the set by some operator of the set, and the following theorem has been established:

The ϕ-subgroup of every group in the equi-transform system is cyclic and of order $2^{\alpha}-1$ *divided by the product of the distinct prime factors of this number.* Incidentally it has also been proved that *every prime factor of* α *is a divisor of the remainder obtained by subtracting unity from some prime factor of* $2^{\alpha}-1$.

UNIVERSITY OF ILLINOIS.